

Joint Collaborative Technology Experiment

Michael Wills^a, Donny Ciccimaro^a, See Yee^a, Thomas Denewiler^b, Nicholas Stroumtsos^c,
John Messamore^d, Rodney Brown^d, Brian Skibba^e, Daniel Clapp^f, Dr. Jeff Wit^f,
Randy J. Shirts^g, Gary N. Dion^h, Gary S. Anselmoⁱ

^a Space and Naval Warfare Systems Center, Pacific, 53560 Hull Street, San Diego, CA, 92152

^b Science Applications International Corporation (SAIC), 3990 Old Town Ave., Ste. 304C, San Diego, CA 92110

^c NAVMAR Applied Sciences Corporation, 1322 Scott St. Ste 104, San Diego, CA, 92106

^d L-3 Communications – MPRI, U.S. Air Force Research Laboratory, 104 Research Road Tyndall AFB, FL 32405

^e U.S. Air Force Research Laboratory, 104 Research Road Tyndall AFB, FL 32405

^f WINTEC Inc., U.S. Air Force Research Laboratory, 104 Research Road Tyndall AFB, FL 32405

^g Aviation and Missile Research Development Center, AMSRD-AMR-BA-TU, B-6264, Redstone, AL 35859

^h Science Applications International Corporation (SAIC), Aviation and Missile Research Development Center, AMSRD-AMR-BA-TU, B-6264, Redstone, AL 35859

ⁱ Science Applications International Corporation (SAIC), 6723 Odyssey Dr., Huntsville, AL 35806

ABSTRACT

Use of unmanned systems is rapidly growing within the military and civilian sectors in a variety of roles including reconnaissance, surveillance, explosive ordnance disposal (EOD), and force-protection and perimeter security. As utilization of these systems grows at an ever increasing rate, the need for unmanned systems teaming and inter-system collaboration becomes apparent. Collaboration provides a means of enhancing individual system capabilities through relevant data exchange that contributes to cooperative behaviors between systems and enables new capabilities not possible if the systems operate independently. A collaborative networked approach to development holds the promise of adding mission capability while simultaneously reducing the workload of system operators. The Joint Collaborative Technology Experiment (JCTE) joins individual technology development efforts within the Air Force, Navy, and Army to demonstrate the potential benefits of interoperable multiple system collaboration in a force-protection application. JCTE participants are the Air Force Research Laboratory, Materials and Manufacturing Directorate, Airbase Technologies Division, Force Protection Branch (AFRL/RXQF); the Army Aviation and Missile Research, Development, and Engineering Center Software Engineering Directorate (AMRDEC SED); and the Space and Naval Warfare Systems Center - Pacific (SSC Pacific) Unmanned Systems Branch operating with funding provided by the Joint Ground Robotics Enterprise (JGRE). This paper will describe the efforts to date in system development by the three partner organizations, development of collaborative behaviors and experimentation in the force-protection application, results and lessons learned at a technical demonstration, simulation results, and a path forward for future work.

Keywords: UAV, UGV, unmanned systems, collaborative behaviors

1. INTRODUCTION

The use of unmanned air and ground systems by military forces has grown dramatically in the past 5 years. In October of 2000 Congress passed Public Law 106-398, the National Defense Authorization Act for FY2001, which established goals for the fielding of unmanned systems. [1] The goals - “By 2010 one third of the aircraft in the operational deep strike force aircraft fleet are to be unmanned,” and, “By 2015 one third of operational ground combat vehicles are to be unmanned.” At the start of Operation Iraqi Freedom (OIF) US military forces had fewer than 200 operational unmanned aerial vehicles UAVs. [2] As of November 2008 there were more than 6,000 UAVs deployed in support of OIF and Operation Enduring Freedom (OEF), flying approximately 400,000 hours in 2008 in support of these operations. As of October 2006 unmanned ground vehicles had responded to over 11,000 Improvised Explosive Device (IED) incidents in theater. [3]

This recent real-world experience with fielded unmanned systems has shown the significant value added that these systems can provide in a wide variety of roles. New Concepts of Operation (CONOPS) and new Tactics, Techniques,

| Report Documentation Page | | | | Form Approved OMB No. 0704-0188 | |
|--|------------------------------------|-------------------------------------|---|---|---------------------------------|
| Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. | | | | | |
| 1. REPORT DATE APR 2009 | | 2. REPORT TYPE | | 3. DATES COVERED 00-00-2009 to 00-00-2009 | |
| 4. TITLE AND SUBTITLE Joint Collaborative Technology Experiment | | | | 5a. CONTRACT NUMBER | |
| | | | | 5b. GRANT NUMBER | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | |
| 6. AUTHOR(S) | | | | 5d. PROJECT NUMBER | |
| | | | | 5e. TASK NUMBER | |
| | | | | 5f. WORK UNIT NUMBER | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SPAWAR Systems Center -San Diego,53560 Hull Street,San Diego,CA,92152 | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited | | | | | |
| 13. SUPPLEMENTARY NOTES SPIE Proc. 7332: Unmanned Systems Technology XI, Orlando, FL, April 14 ? 17 2009 | | | | | |
| 14. ABSTRACT see report | | | | | |
| 15. SUBJECT TERMS | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT Same as Report (SAR) | 18. NUMBER OF PAGES 14 | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT unclassified | b. ABSTRACT unclassified | c. THIS PAGE unclassified | | | |

and Procedures (TTPs) are being continuously explored. Among the lessons learned from these operations, common complaints being fed back from users to the R&D community include a lack of inter-operability between systems, inability to fully exploit potential capabilities through inter-operability, and a lack of system autonomy resulting in high operator workload.

Inter-vehicle collaboration provides a means to address these shortcomings. Collaborative behavior as applied to unmanned systems is defined as two or more unmanned systems working together to accomplish predefined mission(s) with minimal human-operator intervention. It is important to differentiate between a scenario in which multiple unmanned systems utilize inter-system collaboration and other multi-vehicle scenarios. Significant characteristics of multi-vehicle collaboration include the ability for unmanned systems to work as a team, command one another, pass information directly to each other, and make changes to their missions based on that information while being monitored by a human operator. In a non-collaborative environment multiple vehicles operate independently of one another, require one or more operator per system, all sensor data is fed back to the operator(s) for action, and all mission decisions are made by those operators. This non-collaborative environment imposes a high workload on operators and requires a tremendous amount of coordination between them to accomplish even mundane tasks. This high workload non-collaborative environment results in diminished capabilities and decreased situational awareness for battle commanders.

JCTE is a 2 - year effort initiated in December 2007 to develop, refine, integrate, and demonstrate collaborative technology enablers that address needs within multiple Joint Capability Areas (JCAs). JCTE will provide enabling technologies to directly support the following JCAs and Tier 2 capability areas:

- Land operations - joint fires, small unit support, weaponization, navigation, cross country mobility
- Protection - Counter IED, Physical Security, EOD, Counter Sniper
- Special Operations - Tactical Mission Support
- Battlespace Awareness - Persistent ISR

The mission scenario for JCTE is a remote site-security application that demonstrates the capabilities of the component technologies the three partner organizations bring to the project. The JCTE scenario will demonstrate beyond line of sight (BLOS) command and control (C2) of multiple heterogeneous unmanned systems, collaborative roving perimeter patrols by multiple unmanned systems, persistent close-in aerial surveillance by a vertical takeoff and landing (VTOL) UAV supported by in-the-field autonomous launch, recovery, and refueling by an unmanned ground vehicle (UGV), collaborative target ID and lethal engagement, and post-engagement analysis. The scenario requires a high level of interoperability between multiple heterogeneous unmanned systems, enhanced unmanned systems capabilities through the application of collaboration, and a relatively low operator workload given the number of systems employed.

A basic enabling requirement for inter-system collaboration is the use of a standardized communications protocol for C2 of unmanned systems. To date there is no universally accepted consensus for standardization of communications within the unmanned systems community. As a result, most unmanned systems utilize proprietary C2 schemes. The Joint Architecture for Unmanned Systems (JAUS) protocol is an unmanned systems standard that was developed to support interoperability between multiple heterogeneous unmanned systems operating in multiple domains. [4] Though not universally accepted, all of the component technologies employed in JCTE had some level of JAUS compliance when the project started and JAUS provided the best possible collaboration enabler for JCTE. JAUS Reference Architecture version 3.2 (JAUS RA v3.2) was chosen as the communications standard for all unmanned systems and operator interfaces for JCTE because of this ability to support multi-vehicle inter-operability across multiple domains. JAUS is being developed under standards set by the Society of Automotive Engineers under Aerospace Standard - 4 (SAE AS-4).

2.0 BACKGROUND

The JCTE project began with individual developmental efforts at the three partner organizations in the early 2000s. All of these projects were funded by the Joint Robotics Program (JRP, the predecessor to JGRE), incorporated some level of multi-vehicle collaboration, and utilized the JAUS protocol for C2. SSC-Pacific was developing the capability to launch, recover, refuel, and transport a small VTOL UAV on a UGV. AFRL was developing an airborne communications link to extend the operational range of UGVs beyond line of sight. AMRDEC was developing JAUS messages specifically to support collaborative operations and multi-vehicle teaming, and capabilities for multi-vehicle collaboration to conduct lethal fire.

In 2005 the three labs merged these independent projects into a joint effort which the JRP funded for 18 months as the Collaborative Engagement Experiment (CEE) in fiscal years 2005 and 2006. The goals for CEE were to demonstrate the value of collaborative behaviors in accomplishing a complex mission, and to develop a joint framework for future collaborative efforts to avoid independent Army, Air Force, and Navy solutions. [5] While the CEE project did not assemble all the component hardware for a joint collaborative demo due to time and budget constraints, the project did successfully accomplish the following:

- Established a framework under which three services coordinated unmanned systems development efforts to demonstrate joint multi-vehicle collaboration in a real-world scenario.
- Researched ongoing collaborative efforts.
- Conducted user/developer meetings to establish project collaboration goals and a path forward for future work.
- Conducted a task analysis in cooperation with the Soldier Battle Lab at Fort Benning, GA to validate value added of unmanned systems collaboration in a number of common mission scenarios.
- Expanded inter-operability of systems employed by all three labs through use of JAUS.
- Increased component technology maturity levels for all three services.

The JCTE project follows CEE after a one year hiatus to mature component technologies. JCTE goals are an extension of the goals established for CEE – to demonstrate the value added in collaboration between multiple unmanned systems in conducting a complex mission in a real-world scenario.

3.0 JCTE COMPONENT TECHNOLOGIES

3.1 Multi-robot Operator Control Unit (MOCU) (SSC Pacific)

MOCU (Fig. 1) is the operator interface used to provide Command and Control for all of the JCTE unmanned systems. MOCU was developed by SSC Pacific engineers for the simultaneous control of multiple heterogeneous unmanned systems. [6] MOCU operates with unmanned systems across all domains, and is not tied to any specific communications standards or protocols. To date, MOCU has been used to control fixed wing and VTOL UAVs, UGVs, several different unmanned surface vehicles (USVs), and for monitoring of a wide variety of fixed sensors. All of the JCTE unmanned systems communicate with MOCU via a JAUS protocol module.

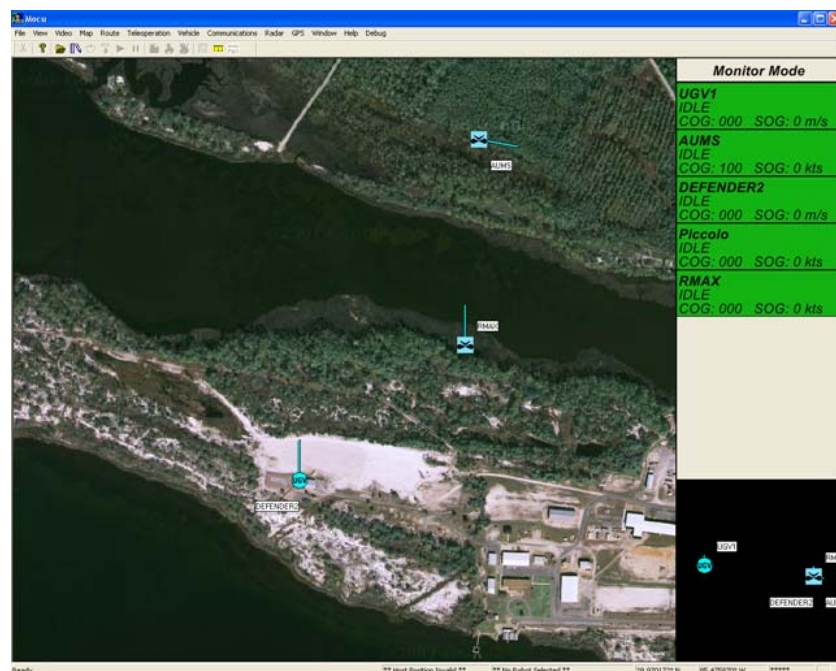


Fig. 1. MOCU screen shot in Monitor mode with two UGVs, two UAVs, and AUMS connected.

MOCU employs a modular, scalable, highly flexible architecture, that allows control and status monitoring of multiple vehicles utilizing differing communications protocols, mapping requirements, and video codecs. It also supports easy expansion by third parties developing new protocol modules. MOCU achieves its modularity through the use of a fixed core module and supporting modules that provide specific functionality. Changes in a system configuration, such as the addition or subtraction of unmanned assets, will require the addition or subtraction of supporting modules. The core module manages data flow between modules and overall operation. MOCU scalability allows great flexibility in hardware configuration, allowing the developer to choose the minimal hardware required and appropriate for a given application.

MOCU supports both control and status monitoring functions for unmanned systems. Status for all vehicles connected to MOCU can be monitored simultaneously, but control can only be exercised over one vehicle at a time. Vehicles displayed in monitor mode appear on a geo-referenced map and basic status info is displayed for each, along with the option to display video from each. For a vehicle in control mode, MOCU has complete control over all vehicle and payload functions, the vehicle status is amplified, and the user interface is configured for that particular vehicle. User interfaces in MOCU, including both input devices such as joysticks and the MOCU GUI, are configured for each vehicle via an XML configuration file. User interfaces for different vehicles can vary dramatically and the use of configuration files to manage these interfaces makes changes to system configuration relatively simple.

3.2 Autonomous UAV Mission System (AUMS) (SSC Pacific)

AUMS (Fig. 2) is a modular, vehicle-borne system to autonomously launch, recover, and refuel VTOL UAVs. [7] A VTOL UAV can provide significant advantages over a fixed-wing UAV in many tactical applications due to its ability to hover and stare or perch and stare at an object of interest. AUMS leverages the ability of a VTOL UAV to autonomously launch and land, and offsets the endurance, range, and payload disadvantages typical of VTOL UAV, via refueling in the field. AUMS can be used as a stand-alone system or mounted on a ground or surface vehicle, manned or unmanned, to autonomously support one or more VTOL UAVs. AUMS mounted on a UGV provides the capability to transport a small UAV into a hazardous area and perform persistent aerial operations without endangering personnel. In a fixed installation, AUMS provides on-demand persistent aerial operations at remote sites without the need to have personnel present at the site. The autonomous nature of the system minimizes exposure of personnel to dangers associated with UAV operations, as well as dangers within the operational environment.

AUMS development began in 2002 as a parallel effort to the DARPA Micro Air Vehicle (MAV) and Organic Air Vehicle (OAV) programs. Development issues with these ducted-fan designs led SSC Pacific to use small helicopters as surrogates to support AUMS development. The current AUMS system used in the JCTE project employs a 20 pound helicopter, the Mongoose UAV, as a surrogate for future fielded VTOL UAVs. The Mongoose is a fully autonomous UAV equipped with a Cloud Cap Technologies autopilot running an adaptive neural-network-based flight controller developed by Guided Systems Technologies. The Mongoose is intended strictly as an R&D platform to demonstrate the AUMS capability, but is equipped with a pan-tilt gimbal that supports an Electro-Optical (EO) sensor to provide basic intelligence, surveillance, and reconnaissance (ISR). Lessons learned in working with the Mongoose should translate to other types of VTOL platforms, including ducted fan designs such as the Honeywell T-Hawk, which is the production version of the MAV.

AUMS is composed of five major subsystems: the launch and recovery platform, the refueling system, the electronics module, the air vehicle, and command and control software. Design goals for the system were:

- Utilize JAUS and MOCU for AUMS, the UAV, and the UGV to support automation of the launch, recovery, and refueling processes and maximize collaboration between the three to minimize operator workload.
- Maximize landing platform size without impacting host vehicle footprint – i.e. platform should not exceed the host vehicle length or width.
- Provide a secure means of transporting the UAV. AUMS can transport a UAV over significant distances and through potentially hostile environments so a means of securely attaching the UAV to AUMS is required.
- Easy integration to the host vehicle. AUMS is a fully self contained system capable of operating stand alone. As such it requires no significant software modifications and minimal hardware modifications to the host vehicle.

- Minimal modifications to the air vehicle. Typically modifications are confined to landing gear and addition of the refueling coupler. If the UAV flight control system does not provide sufficient navigation precision to reliably and consistently land safely on the platform, changes to the flight control system may be required.
- Modular. Easy to modify the system to suit host and air vehicle needs.
- Safety systems to detect and respond to fuel leakage or fire.
- Flexible fuel source and type as required. The refueling module incorporates a dedicated fuel tank, or can tap into the host vehicle fuel supply as required.
- The system is compatible with gasoline or heavy fuels as required by the air vehicle.
- Provides for partial or complete refueling as required by payload and mission considerations.

AUMS provides JCTE a persistent, on demand, local airborne ISR capability at a remote location as compared to a more traditional approach utilizing fixed wing UAV assets which must transit to and from a support base to the remote site.



Fig. 2. HMMWV UGV host vehicle, AUMS, and the Mongoose UAV.

3.3 RMAX UAV, Unmanned system Communication Repeater (UCR), and Link Management System (LMS) (AFRL)

The RMAX UAV (Fig.3) is a COTS rotary wing VTOL platform with a 10.2 ft main rotor diameter and a 66 lb payload capacity. For JCTE, the RMAX carries the Unmanned Systems Communication Repeater (UCR) payload which provides the BLOS communications link for all of the unmanned systems used in the experiment.

The RMAX employs a COTS WePilot autopilot system consisting of an autopilot control unit, radio link, and a ground control station. The autopilot control unit receives input from onboard sensors (gps, rate gyro, and engine rpm) and directs the native Yamaha flight controller based on ground control station commands or stored waypoint paths. The WePilot uses a single 2.4 GHz, 100 mW radio link and single antenna pair for both data and video communications. An independent communications link employing a 72 MHz radio provides backup for manual pilot in the loop control.

The UCR is a bi-directional RF digital data repeater developed to support BLOS networked communication between one or more operators and one or more unmanned systems (UMS). The UCR extends the effective range of operation for a UMS communication network based on 802.11 WiFi to distances that are beyond visual range. This is accomplished by placing a communication repeater node in the air on a UAV as a self contained payload. The UCR provides an airborne link between the MOCU local network and one or more UGVs. The overall link is actually implemented via two separate links, an L-band between the MOCU network and UAV, and an S-band between the UAV and the UGVs. The L-band link is implemented as a FM telemetry uplink/downlink operating on two separate frequencies. The S-band link is essentially WiFi conforming to 802.11 b/g.

The UCR capability was originally developed and demonstrated with the Comm-Payload carried internal to a small fixed wing UAV in 2003. For the JCTE effort this capability was modified to provide performance improvements as well as for test and demonstration on a rotary wing UAV. Technical objectives achieved by the UCR under the JCTE effort included the following:

- Integrate/test the Comm-Payload on a rotary wing platform.
- Reduce operator workload.
- UCR performance verified out to 15 miles.
- Data throughput sustained at 6Mbps.
- Simultaneously support multiple operators working from multiple MOCUs.
- Simultaneously maintain BLOS operations of multiple UGVs.
- Improve UCR L-band link performance through the integration of a commercial high-gain tracking antenna system incorporated at the MOCU end of the link.

The Comm-Payload, the airborne component of the UCR, is installed in a tubular pod 24" long by 7.5" in diameter. The pod weighs 25 lbs. and is powered by 28VDC @ 7.5A maximum power consumption. The fully self contained Comm-Payload pod is mounted to the underside of the RMAX fuselage between the landing gear legs.



Fig. 3. RMAX Rotary Wing UAV with UCR payload.

The Link Management System (LMS) is a software module developed to automate management of dynamically created mobile and fixed wireless networks supporting UMS operations. The LMS uses a-priori knowledge of performance parameters associated with all participants, fixed and mobile, that may join the network. This knowledge along with dynamically updated position information for each participant is used to compute the region of effective communication for each transmitting/receiving node. Using well defined and tested RF path-loss algorithms, the LMS computes the effective communication region for each participant in the network. Overlapping coverage areas identified by the LMS represent regions in which one or more participants are able to communicate with each other. The output of the LMS can be used for dynamic path planning and intermittent or lost communication response management.

During the JCTE effort, the LMS was effectively used to determine the optimum location for placement of the UAV carrying the UCR Comm-Payload. The LMS determined the effective communication region for the L-band link between MOCU and the UAV carrying the Comm-Payload, and again for the S-band link between the UAV and ground vehicles. Communication equipment parameters (i.e. Tx power, Rx sensitivity, antenna gains, etc.) for each participant in the network were loaded into a configuration file that was read by the LMS upon startup. Participant position reports

were constantly monitored by the LMS, which was connected to the JAUS network. Based on these inputs, the LMS computed the optimum location for the RMAX UAV in order to establish and sustain communications between the OCU and UGVs. This position was reported across the JAUS network to the RMAX controller as a fly-to waypoint. When enabled, the RMAX would automatically fly-to the optimum position reported by the LMS. This capability was tested, evaluated, and demonstrated during the JCTE effort.

3.4 Defender UGV (AFRL)

The patrol/engagement UGV used for JCTE is the “Defender” (Fig. 4) developed by the Robotics Research and Development Group at AFRL. This platform performs the challenge, response, delay/denial and neutralization role in the experiment. The Defender is capable of high speeds (up to 35 mph), can negotiate wooded areas, is “zero radius” turn capable, and can travel through rough terrain (at reduced speeds). The platform has a minimum mission endurance of 6 hours.

The vehicle is based on the Land Tamer II 6X6, a diesel-powered vehicle developed by PFM Manufacturing. The vehicle comes equipped with a 17-gallon fuel tank, giving an estimated 17-hour run time at 50 percent power. The engagement platform has a color camera system for video feedback as the primary driving reference. It has a strobe/flashing light system, a speaker/microphone for subject interaction, and lethal weapon systems incorporated into the base platform. The lethal weapon employed is either the M-16A2 rifle or M-240/M249 machinegun. The lethal weapon is mounted in and controlled with a Telerobotics XROWS™ Remote Operated Weapon System. JCTE employs two Defenders.



Fig. 4. Defender Engagement System.

3.5 Pointing Algorithms (AMRDEC)

The pointing algorithms originated from the Computer-Aided Fire Control program (CAFC), which began in January 2005 to develop technologies with potentially immediate application to remote weapons operation. The focus of CAFC was to develop technologies to reduce warfighter workload and to improve remote weapon performance by automating the targeting of a weapon. CAFC included a software interface that utilized a ballistics library that provided ballistic corrections given the physical properties of the bullet and atmospheric conditions. It also employed a pointing algorithm which computes the azimuth to target of a turret given the GPS coordinates of the turret and the target. JCTE is utilizing the pointing algorithm aspect of CAFC to target potential threats using AFRL’s Defender platform, then adding upon CAFC capability by passing targets between unmanned systems.

The pointing algorithm allows a collaborative team to effectively monitor a threat or area of interest by slewing a turret, which may have a camera or a weapon attached, to a specified target. This algorithm computes the azimuth to target by

taking into account the yaw, pitch, and roll of the vehicle on which the turret is mounted and the GPS coordinates of the turret and the target. The pointing algorithm is an effective method to use for the targeting and overwatch of threats, but because it assumes that a bullet will fly in a straight line it is not accurate enough to provide precise engagement capabilities.

Precise engagement in a collaborative environment is enabled by the ballistic library algorithms. The ballistic library algorithms (Fig. 5) compute corrections based on the physical characteristics of the weapon and the round, and on the present atmospheric conditions. Physical properties such as the mass, diameter, form factor, and muzzle velocity are combined with atmospheric conditions such as temperature, pressure, humidity, altitude, and crosswind to produce a superelevation of the bore in order for the bullet to hit the target.

The ballistic library has been validated with a variety of projectiles and velocity regimes. It has been validated at supersonic velocities with a 7.62-mm round at distances from 100 m to 800 m, at nearly sonic velocities with a MK-19 40 mm grenade launcher from 100 m to 300 m, and at subsonic velocities with a FN303 less-than-lethal projectile from 10 m to 100 m. In a collaborative environment this allows precision engagement from a variety of platforms.

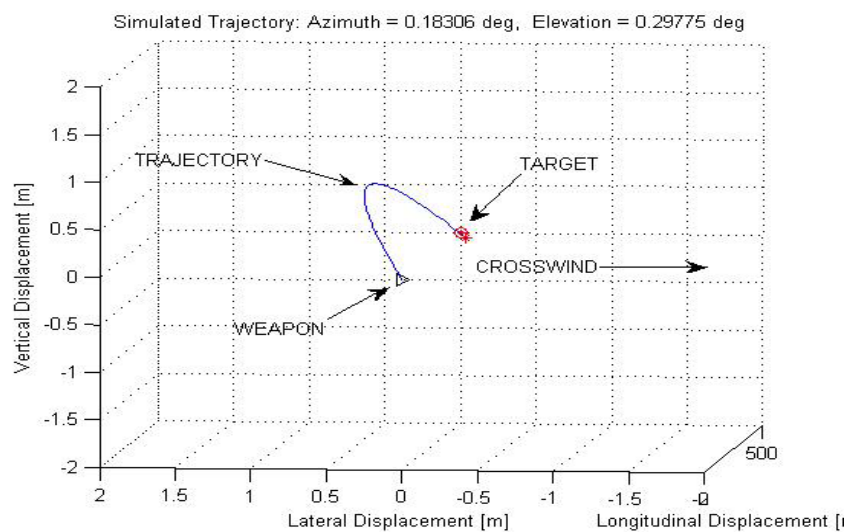


Fig. 5. Ballistic Algorithm.

3.5 AUMS Host Vehicle – Unmanned HMMWV (AMRDEC)

A robotic High Mobility Multipurpose Wheeled Vehicle (HMMWV) was designated as the AUMS host vehicle. The vehicle is a M1097A1 HMMWV, which is a high payload configuration intended to transport equipment, material, and personnel. The robotic HMMWV was selected for its payload capacity, size, and familiarity within the military community. It has been converted to run in both tele-operation and manual driving modes. In tele-operation mode, the AUMS host is software limited to drive 15 MPH forward and 5 MPH in reverse. The operator may use the brake, emergency stop, and start/stop the engine. The operator may also change gears from forward, neutral, and reverse. The steering is the same Ackermann steering system as a standard HMMWV. Forward and rear driving cameras are provided on the AUMS host, and the video feed automatically changes from the forward to the rear driving camera when the operator changes the gear from forward to reverse and vice-versa.

The AUMS host vehicle and the AUMS system are implemented completely independent of each other, except for the physical interface between the two systems. Physical integration of the two systems amounted to installing the AUMS platform and refueling module on a previously existing pedestal on the host, and locating AUMS and host vehicle antennas on the host such that the systems did not interfere with one another, nor with the flight of the Mongoose UAV.

To achieve MOCU compatibility, a portion of the command class-core subgroup of the JAUS/AS-4 message set was integrated into the robotic HMMWV system. The implemented messages include: Request Component Control, Release Component Control, Confirm Component Control, and Reject Component Control.

3.6 JAUS Teaming Messages (AMRDEC)

One of the goals for JCTE is to demonstrate that unmanned systems teams can be formed to collaboratively accomplish mission requirements. Teaming messages are meant to enhance the collaboration capabilities of a team of robots. They allow a robot that has been given a specified mission, (i.e. the Team Leader) to query other robots within communications range. The team leader sends out a broadcast to find robots with capabilities that may help accomplish the mission. When the team leader receives the neighboring robots capabilities, the Team Leader or an operator may choose which robots to allow on the Team. Once they have joined a Team, these robots may utilize their available capabilities to assist in accomplishing the Team Leader's mission. Once the mission is accomplished, the Team is disbanded and they wait for another mission to be requested. A group of JAUS teaming messages was created as follows:

- Code DA00h: Request Team Leadership/Membership.
- Code DA01h: Reply Team Leadership/Membership.
- Code DA02h: Release Team Membership.
- Code DA03h: Add Team Member.
- Code DA04h: Remove Team Member.
- Code EA05h: Query Team Membership.
- Code FA05h: Report Team Membership.
- Code DA06h: Request Peer Connection.
- Code DA07h: Set Peer Connection.
- Code DA08h: Terminate Peer Connection.

Due to time, budget, and capabilities constraints the teaming messages were not fully implemented in all of the JCTE unmanned systems. As a result, it was decided to have all JAUS commands initiated from MOCU, so the Team Leader role will be taken by the MOCU forming the team. The teaming structure will have the primary MOCU as team leader and request membership from (1) secondary MOCUs, (2) Base Position Sensor, and (3) all the UGVs and UAVs.

4.0 JCTE ARCHITECTURE

The initial task of integrating all the individual systems involved establishing a common communication interface, which included all the messages (commands and data), and the communication scheme to be used. The messaging scheme selected was that specified under the JAUS RA v3.2. A JCTE JAUS Interface Design Document (IDD) was drafted that included (1) the communication scheme (transport protocol, network configuration and wireless communications setup), and (2) the details of all the JAUS messages supported by each system. The goal was for each system to be compliant with the IDD, tested independently using MOCU, and then tested together with all the other systems.

The main transport protocol for all the JAUS traffic was Ethernet. Both wired and wireless Ethernet links were used. On the C2 end, three MOCUs and one LMS GUI display were on a wired network connected to the base side of the UCR. The remote side of the UCR, which is carried by the RMAX, was bridged to the individual ground systems (which included two Defender UGVs, one AUMS Host UGV, and the RMAX Ground Control Station) using wireless Ethernet (802.11b/g).

The IP scheme used had all the systems under the same subnet. A block of IP addresses were assigned for each system. A list of all the IP addresses of systems on both the remote and base sides were stored in the UCR base and remote PCUs as an access-control list. Only data to and from the systems on the list are allowed to pass through the Repeater, thus preventing unwanted traffic.

For the wireless Ethernet link, the radio on the UCR remote side was set-up as an access point. The radios on the remote ground systems (UGVs and the RMAX Ground Control Station) were set-up as wireless clients. All the data traffic from the ground systems passed through the UCR access point first, and the effective bandwidth was shared by these ground systems.

Prior to JCTE, all of the systems had some level of JAUS compliance and some of the individual systems were already JAUS RA v3.2 compliant. The experience in using JAUS as the common messaging interface served well in selecting the existing messages needed, plus drafting user-defined messages specific to certain functions and platforms. The specific details of all these messages are in the JCTE JAUS IDD v1.0. The types of JAUS messages according to function are: (1) Platform Mobility and Control, (2) Target Detection and Track Passing/Pointing, (3) Link Management System, and (4) Teaming. The last three were the main areas of collaboration between the systems. Remaining integration tasks included ensuring all systems were compliant with the JCTE IDD, frequency management, and bandwidth management.

5.0 TEST AND INTEGRATION SESSIONS

There were three integration test sessions conducted, which were scheduled based on system readiness, with the last test session culminating in the technology demonstration. The first integration session goals were: (1) verify the IP scheme and check the network configuration using a wired connection, (2) verify the vehicle/subsystem discovery process using MOCU, (3) test and verify critical feedback including position, velocity and status, and (4) test video and measure bandwidth utilization. Most of the testing in session one was conducted with software simulators in place of actual system hardware.

The second integration session was an extension of the first, utilizing more hardware in place of simulation and introducing the wireless communication links. The main goals of the second integration session were: (1) verify network configuration using both wired and wireless connection, (2) using MOCU, verify discovery, status and feedback of vehicles, (3) test LMS, (4) test Targeting and Pointing, and (5) test auto tracking antenna for UCR L-band link at short and long ranges.

The third scheduled integration session was the final stage in the integration process and ended with the technology demonstration. This was the first time that all the individual system hardware was together for total system integration. The complete demonstration scenario was tested in this session.

5.1 Test and Integration Sessions Results and Lessons Learned

There were no significant issues uncovered in the first integration session.

Session two issues uncovered were:

- In testing communications with the ground vehicles, antenna placement on the AUMS Host UGV was found to be critical. The AUMS host was prone to lost communications until an appropriate antenna configuration was determined through experimentation.
- In testing with MOCU, if each vehicle was tested independently, there were no apparent issues. When all the vehicles were turned on at the same time, there were problems in the discovery process between the Defender vehicles and the AUMS Host UGV. There would be constant rediscovery that would cause the AUMS Host UGV computer to drop out. This problem was only partially resolved and will require further development and testing.
- The BLOS tracking antenna system was successfully tested at a range of 0.5 miles but there was insufficient time during integration session 2 to conduct any testing at longer ranges.

Targeting and Pointing were tested in session two using MOCU and Defenders 1 and 2. Defender 2 set a target using its laser range finder to sight an object. The target would appear as an icon on the map on MOCU. Pointing was performed by using MOCU to send the position information of that target to Defender 1, commanding the selected pan/tilt camera to point at that location. Results showed that the pointing was within 3 degrees of the actual target.

Session three issues uncovered were:

- With all the hardware in place there were significant frequency management issues that were partially solved by changing 802.11 channels and changes to the RMAX WePilot communications radio and Mongoose UAV video transmitter. Ultimately these conflicts were not entirely resolved. For safety reasons, both UAVs could not be flown simultaneously during the demonstration. This problem will be addressed before the FY09 Warfighter experiment.

- The BLOS C2 was initially problematic at the 4 mile experiment range due to an artificially low ceiling of 500 meters for the UAVs, which imposed a very low elevation angle for the tracking antenna. The low elevation angle was obstructed by a tree line near the tracking antenna. This problem was addressed by relocating the tracking antenna.
- There were minor problems on the RMAX end of the long link that were solved by relocating antennas on the UAV.

6.0 SIMULATIONS

The test scenario for JCTE is a force-protection application in which unmanned systems were used to secure a remote airfield. There were nine separate test cases defined to evaluate the potential benefits of JCTE technologies and collaboration under varying conditions. The test cases were defined as follows:

Reconnaissance and Patrolling, non-collaborative technologies - JCTE Scenarios #1 - 3

- CASE 1: Base Case – Perimeter Defense - Current cooperative technologies, range 1 – 2 km LOS.
- CASE 2: Base Case - Respond to Hostile Threats - Current cooperative technologies, range 1 – 2 km LOS.
- CASE 3: Base Case - Recon/Patrolling - Current cooperative technologies with communications relay, extended range.

Extended Perimeter Defense with added Collaborative capabilities - JCTE Scenarios #4 - 8

- CASE 4: Test Case - Recon/Patrolling - Collaborative technologies, extended range with communications relay and Link Management System (LMS).
- CASE 5: Test Case - Recon/Patrolling - Collaborative technologies, extended duration using the AUMS, 30 minutes UAV sortie duration.
- CASE 6: Test Case - Recon/Patrolling - Collaborative technologies, extended range with communications relay and LMS, extended duration employing AUMS, 30 minutes UAV sortie duration.
- CASE 7: Test Case - Respond to Hostile Threats - Collaborative technologies, target location passing using LMS and pointing/cueing. Unmanned systems will be utilized to induce hostile target delay and denial. Targets will be neutralized using simulated lethal and/or non-lethal means to gain insights into experimental gains in efficiency realized through collaborative targeting/cueing.
- CASE 7A: Test Case - Respond to Hostile Threats – Excursion – same as Case 7 except HMMWV, AUMS, and Mongoose UAV forward deployed to minimize transit time.
- CASE 8: Test Case - Recon/Patrolling & Respond to Hostile Threats - Collaborative technologies with future capabilities.

JCTE employed simulations for all nine cases and used trend analysis to evaluate results. The modeling and simulation effort focused on being able to visualize the JCTE system of systems in an operational context and describe and assess the potential military utility of the various capabilities. The team used the System Effectiveness Analysis Simulation (SEAS), which is a multi-agent, net-centric simulation model that is able to represent future systems, concepts of operations and doctrine. The JCTE capabilities were incorporated into programmable agents behaving in accordance with the JCTE study cases. The systems modeled in the simulation included small generic rotary-wing UAVs with a 30-minute flight time. The same type of UAV served both as the reconnaissance platform and the platform for the LMS and the communications relay. For cases 5 - 8 the UAV had the capability to land on an AUMS-equipped vehicle and refuel. Defender UGVs armed with an M-240B machine gun provided the ground reconnaissance and response capabilities. Additionally, a ground surveillance radar (GSR) with a detection range of 10 km was modeled and used in the simulations.

The modeling and simulation scenario used these simulated unmanned systems for base defense. The security forces employed the system of systems covering a limited sector in a layered defense. Operations were continuous in a 120° sector with named areas of interest (NAIs) out to just beyond 10 km. The simulated threat involved small armed teams moving by foot toward an airfield with the intent of causing damage to military equipment or personnel casualties. Once a threat was detected, the unmanned systems maneuvered to identify and intercept the threat.

A set of fifty simulation runs for each case produced data for trend analysis, which when compared across test cases, indicated a very significant benefit to employing JCTE technologies. Without collaborative technologies, the UGVs and

UAV had to remain within line of sight and were only able to observe NAIs near the installation. Additionally, the UGVs were only able to intercept the threat forces when they were already close to or within the perimeter. Interception at greater distances would have to be performed by security forces that would then be exposed to greater risk.

Adding collaborative capabilities increased the operational range of the unmanned systems as well as the time that those systems could continue to perform at those distances. This enabled the friendly forces in the scenario to execute a much more extensive and comprehensive collection plan covering a greater number of NAIs. This extended operational range also enabled the friendly forces to intercept threat forces at a much greater distance from the base perimeter.

Figure 6 below summarizes the results of those cases involving threats with Case 2 being a baseline for comparison and Cases 7 and 7A indicating the benefits of the collaborative technologies involved with the JCTE effort. The bottom line was that the collaboration technologies provided security forces greater flexibility to conduct reconnaissance and surveillance at greater distances over a much larger area. Collaboration also provided security forces with the ability to observe and engage threats at a greater distance from the base.

| | Metric | Current Non-Collaborative (Case 2) | JCTE Capability (Case 7) | JCTE Capability with Forward- Deployed AUMS (Case 7A) | Trend |
|--|---|--|----------------------------------|--|---|
| Extended Range | Maximum Range | 2 km LOS | 11 km (5.5 x current) | > 11 km (>5.5 x current) | UGVs can operate farther from base and engage targets at greater standoff distances. |
| | Average Distance from BDOC to Intercept Threat | 2.1 km | 5.0 km (>2.3 x current) | 9.1 km (>4.3 x current) | |
| Extended UAV Flight Time | # Sorties / 8-hr period | 10 | 12* (+20% over current) | 12* (+20% over current) | UAV can spend more time aloft at greater standoff distances. *See note below. |
| | Flight Time / 8-hr period | 5 hr | 6 hr* (+20% over current) | 6 hr* (+20% over current) | |
| | Time on station at 7 km / 8-hr period | 1 hr 6 min | 2 hr 36 min* (2.35 x current) | 6 hr* (5.4 x current) | |
| Increased Lethality / Reduced Target Engagement Times | Time Threat Operated w/o Being Engaged | 9 hr 14 min | 5 hr 59 min (65% of current) | 1 hr 24 min (15% of current) | Threats were disrupted sooner and friendly losses decreased. |
| | % of Runs When Threat Was Unable to Inflict Damage / Casualties | 9% | 21% (+12% over current) | 87% (+78% over current) | |
| | Average Friendly Losses | 5.3 | 1.2 (22.6% of current) | 0.1 (0.2% of current) | |
| Notes | *The simulation used a factor for the AUMS refuel time of 10 minutes. Actual experience is demonstrating an AUMS refuel time of 4 minutes. Using 4 minutes, the UAV could fly 14 sorties (40% improvement), total flight time over an 8-hr period of 7 hrs (40% improvement), and a time on station at 7 km of 3 hr 3 min (2.77 x current). | | | | |

Fig. 6. Summary of JCTE Simulation Results.

7.0 THE JCTE DEMONSTRATION

Testing with hardware was confined to test case 7A due to time, budget, and resource constraints. Testing concluded with a demonstration at the end of the third integration test session. This was conducted over a 2 week period in October 2008 at Tyndall AFB in Florida. The demonstration site was the Silver Flag facility, an unused runway located south of the main airfield at Tyndall. Silver Flag is typically used for a variety of testing and exercises and includes a concrete runway 6,000 ft. long, a perimeter road around the runway with some scattered buildings, and forested surroundings. The site underlies Restricted Airspace R-2905B making airspace access for the two UAVs relatively simple. A simulated Base Defense Operations Center (BDOC) was setup at the AFRL Robotics Facility located approximately 4 miles from the Silver Flag test site. The BDOC hosted the MOCU operators for all of the unmanned systems used in the experiment, the UCR Comm-Package, and UCR tracking antenna.

A conceptual description of the implementation of the unmanned systems for the Case 7A demonstration follows. The RMAX UAV equipped with the UCR Comm-Payload hovers above the Silver Flag test site to provide the BLOS communications link between the MOCU operators at the BDOC and the unmanned systems at Silver Flag. The LMS evaluates UGV positions at Silver Flag and positions the RMAX to an optimum position for best communications via waypoints. The AUMS host vehicle serves as a remote base of operations for the Mongoose UAV, which provides an airborne persistent on-demand ISR capability for system operators at the BDOC. The AUMS host vehicle can be remotely positioned anywhere on the Silver Flag site as required by operators. The Mongoose UAV returns to the AUMS host for refueling and redeployment as required. The Defender vehicles provide roving patrols of the airfield and an armed response capability should a threat be detected by any of the unmanned systems. An intruder is introduced to the site and Defender #1 detects the intruder. However Defender #1 does not have a clear line of sight to employ its weapon due to obstructions in the background. Defender #1 passes the target information to MOCU which in turn passes the target info to Defender #2. Defender #2 in an unobstructed position simulates engaging the intruder. The Mongoose flies overhead to provide operators at the BDOC video of the engagement for situational awareness and post engagement analysis. In this scenario the initial target designation could just as easily come from the Mongoose UAV or from either Defender UGV.

As mentioned in Section 5.0 there was a frequency management issue that precluded flying both UAVs simultaneously for safety reasons. As a result, the planned scenario was modified and conducted in two parts. Part 1 of the demo was much as described in the previous paragraph with the Defenders patrolling, encountering and engaging an intruder, and passing targeting info, all controlled over the BLOS C2 link. The only deviation was the inability to fly the Mongoose to provide aerial ISR. Part 2 was a standalone demonstration of the AUMS, AUMS host, and Mongoose UAV conducted locally at Silver Flag. A fully autonomous launch from the HMMWV was followed by an ISR mission, autonomous recovery on the HMMWV, a refueling sequence, and a second launch, ISR mission, and recovery.

8.0 SUMMARY AND PATH FORWARD

JCTE brought together a number of complimentary capabilities and integrated them relatively rapidly by utilizing JAUS as a communications protocol and MOCU as a common C2 system. These capabilities were employed to demonstrate a real world application – security of a remote site with a number of unmanned systems operating collaboratively. Simulations were used to establish a base capability and to show capability improvements as more systems were introduced operating in a collaborative fashion. The simulations show a dramatic improvement in capability as well as a reduction in operator workload as more collaborative capabilities are introduced.

A demonstration of Case 7A, the most complex of the 9 cases achievable with the technology available, was conducted. The Case 7A demonstration successfully showed that multiple unmanned systems could be employed remotely via a BLOS communication link to provide site security. Collaboration between the LMS and RMAX maintained optimum link quality in real time for the duration of the demonstration. The Defender engagement platforms autonomously patrolled the site and upon detecting an intruder, worked in collaboration with each other and MOCU to engage and neutralize that intruder. Three operators running three instances of MOCU at the BDOC were able to monitor and control three UGVs and a UAV simultaneously while all were seeing a Common Operating Picture. A VTOL UAV ISR asset was launched and demonstrated the ability to autonomously extend its on-station duration by landing on a UGV, refueling with engine running, and relaunching to maintain a persistent ISR capability with minimal down time. This persistent ISR capability is enabled through the use of JAUS, MOCU, and air-ground unmanned systems collaboration.

Improvement for FY09 will include addressing frequency management issues, more fully implementing teaming to increase collaboration, and increasing reliability and capability of some of the unmanned systems. Implementing these improvements should allow greater capability while simultaneously further reducing operator workload. JCTE for FY09 plans to conduct a warfighter experiment in the September timeframe, details of which are still being determined.

ACKNOWLEDGEMENTS

JCTE is supported by the Office of the Secretary of Defense, Joint Ground Robotics Enterprise. SPAWAR would like to acknowledge the support provided by Guided Systems Technologies in the development of the Mongoose UAV.

REFERENCES

- 1) 106th Congress of the United States, Public Law 106–398 Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, October 30, 2000, <http://www.jointrobotics.com/congressdocs.php>
- 2) Dyke Weatherington, "Unmanned Aircraft Systems", Marcus Evans UAV Conference, 18 November 2008
- 3) Unmanned Systems Roadmap 2007 -2032, <http://www.jointrobotics.com/library02.php>
- 4) Joint Architecture for Unmanned Systems, <http://www.jauswg.org/>
- 5) Katherine Mullens, Bradley Troyer, Robert Wade, Brian Skibba, Michael Dunn, "Collaborative Engagement Experiment," SPIE Proc. 6230: Unmanned Systems Technology VIII, Defense Security Symposium, Orlando, FL, April 18-20, 2006.
- 6) D. Powell, G. Gilbreath, M. Bruch, "The multi-robot operator control unit (MOCU)," SPIE Proc. 6230: Unmanned Systems Technology VIII, Defense Security Symposium, Orlando, FL, April 18-20, 2006.
- 7) Mike Wills, Aaron Burmeister, Travis Nelson, Thomas Denewiler, Kathy Mullens, " The Development of a UGV-Mounted Automated Refueling System for VTOL UAVs," SPIE Proc. 6230: Unmanned Systems Technology VIII, Defense Security Symposium, Orlando, FL, April 18-20, 2006.